Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 25 April 2022 - Monday 16 May 2022

Supervised hours 5 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part A

You must have:
Risk_Assessment.rtf
Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- Learners must only have access to **Part A** during this supervised assessment period.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- **Part B** materials must not be accessed during completion of **Part A**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer all activities.

Information

- The total mark for this Part is 43.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete **Part A** on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in **Part A** but cannot provide any guidance in completion of the activities.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is **not** permitted.
- Learners' work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely, and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A**, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work.

The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 18 May 2022.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities. Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is **not** allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in **Part A** but cannot provide any guidance in completion of the activities.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within this folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

The Gangala Aventurparko

The Gangala Aventurparko is in the country of Varma Loko and is one of several tourist attractions owned by Varma Loko Leisure Parks (VLLP).

Gangala Aventurparko has a mix of water activities, rides, shops, and cafes. The area is designed with a jungle theme.

VLLP is going to improve all its parks. Gangala Aventurparko is the pilot project. The improvements will require a new IT system.

The work will be managed by the Project Manager, Viro De Ordoni.

Figure 1 shows a map of the park and the area around it.

The private beach to the north is owned by VLLP and can only be accessed via the park. The other three sides have a secure perimeter fence separating the park from undeveloped forest. Visitors arrive on an access road which ends at a car park near the entrance.

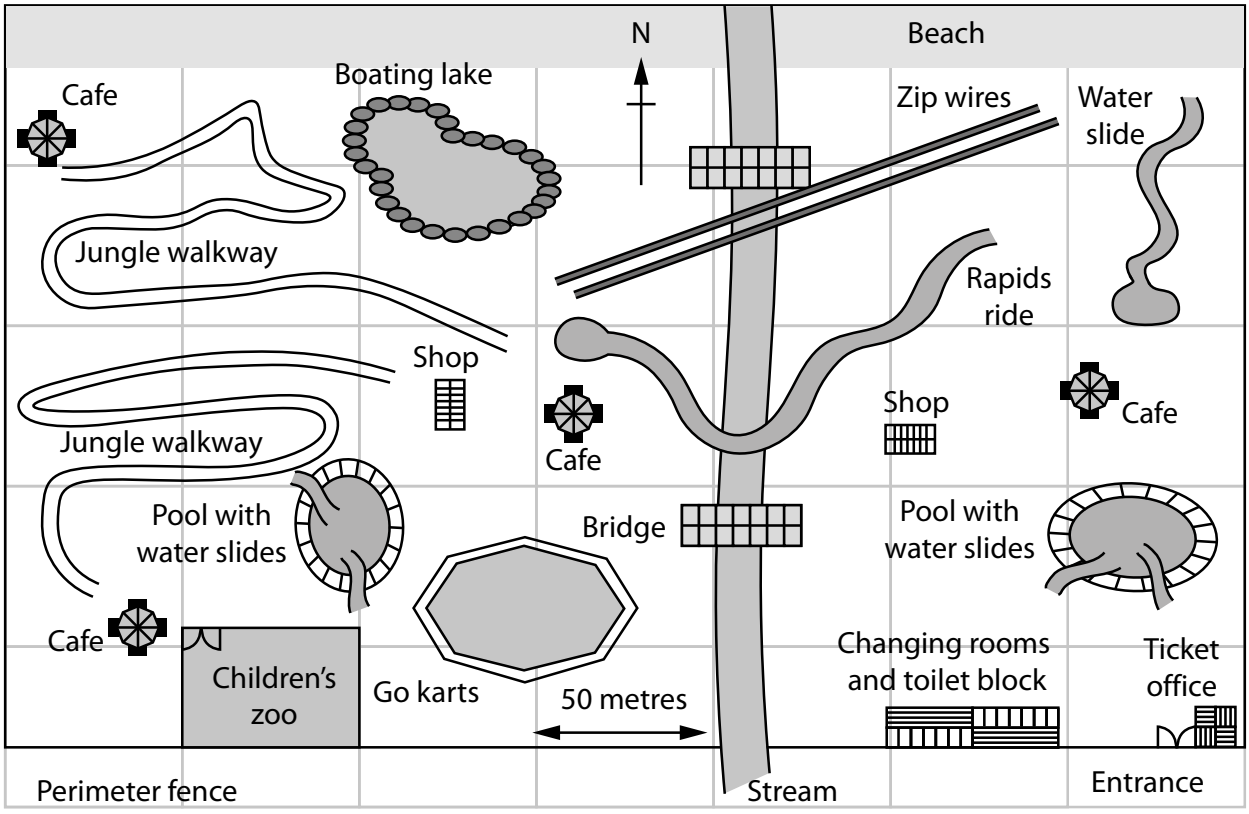

Figure 1

At the moment, visitors buy tickets on entry and then pay extra for some of the attractions, such as the Zip wires and Children's zoo.

Payment at the ticket office, shops and cafes is by cash or card. Payment at the attractions is only by cash.

VLLP wants to make payment more convenient for visitors and cheaper to run for the company.

The plan for payment is to give each visitor a wristband containing an RFID chip. RFID chips use near field communication (NFC) to link to a chip reader connected to the local area network (LAN).

The wristband will be linked to the visitor's personal VLLP account. The account can be preloaded with credit at the ticket office or at one of the shops.

Visitors may also link their account to a credit card so that they do not need to preload. Payment is then taken from their credit card when the visitors leave the park.

When visitors want to use one of the paid attractions or buy something at a shop or cafe, their RFID chip will be read. Payment is then taken from the visitor's VLLP account.

Figure 2 shows the plan for the new IT system at the park.

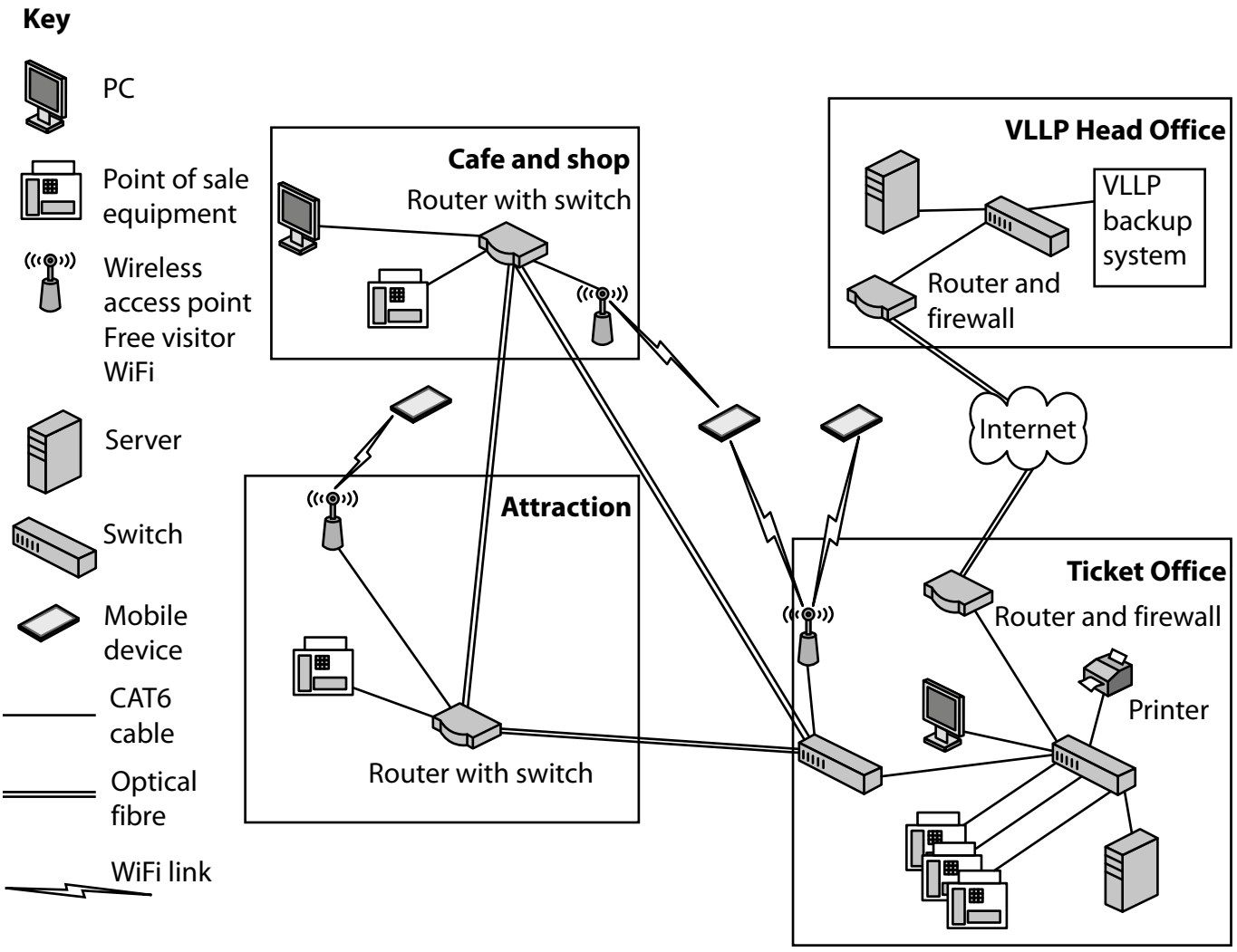

Figure 2

Viro De Ordoni is an experienced Project Manager. He has previously managed several successful projects for VLLP. He has a good knowledge of IT matters but relies on managing other people's expertise rather than trying to do everything himself.

Viro has hired you to look at the plan and advise on cyber security and incident management.

Development plan

At a meeting with Viro you establish that:

1. All current IT equipment will be replaced with items as shown in the network plan, **Figure 2**.
2. Free WiFi will be available for guests throughout the park.
3. A wireless access point will be placed in the ticket office and at each shop, cafe and attraction.
4. The ticket office will be connected to each shop, cafe and attraction by optical fibre.
5. All other internal cabling will use CAT6 cable.
6. Viro is concerned about WiFi security and access being available from outside the park.
7. Employees at fixed locations, such as shops, will use an internal VOIP system for communication.
8. Roving employees such as security staff will use two-way radios.
9. Backups will be sent overnight to VLLP Head Office.
10. The network PCs and servers will run the latest, professional version of Windows.
11. Viro is concerned about disruption caused by the automatic Windows update system.
12. The point of sale equipment in the ticket office, shops and cafes will accept cash or cards.
13. The point of sale equipment elsewhere will only use the RFID wristband for payment.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

Viro has hired you to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS
TOTAL FOR PART A = 43 MARKS